STATE OF ALABAMA

Information Technology Standard

Standard 670-05S1_Rev A: Intrusion Detection and Prevention Systems

1. INTRODUCTION:

Intrusions may be the result of attackers accessing the systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. Intrusion detection and prevention systems automate the process of intrusion monitoring and analysis. A properly configured Intrusion Detection System (IDS) can detect unauthorized system access and alert personnel who can contain and recover any resulting damage. An Intrusion Prevention System (IPS) provides another layer of access control, similar to a firewall, and properly configured can deny unauthorized and potentially malicious activity. IDS and IPS technologies offer many of the same capabilities. Accordingly, for brevity the term *intrusion detection and prevention system* (IDPS) is used here to refer to both IDS and IPS technologies.

2. OBJECTIVE:

Establish the requirements for the deployment of intrusion detection and prevention systems on State of Alabama computer and network resources.

3. SCOPE:

These requirements apply to all State of Alabama networks and application servers.

4. REQUIREMENTS:

> *Policy: State of Alabama organizations shall, in accordance with applicable standards, position intrusion detection and/or prevention capabilities on networks and application servers commensurate with classification and criticality of data processed based on level of risk to unauthorized access.*

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), State of Alabama organizations shall implement the following requirements pertaining to intrusion detection and prevention systems.

4.1 IDPS DEPLOYMENT

Use multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity. There are four primary types of IDPS technologies—network-based, host-based, wireless, and network behavior analysis (NBA).

Use a combination of network-based and host-based IDPS for an effective IDPS solution.

Utilize Host-based IDPS on application servers that process and store information whose confidentiality, integrity and availability are deemed crucial and where unauthorized access would be detrimental to the State of Alabama.

Utilize Network-Based IDPS on:

- Internet-connected gateways positioned inside the firewall to monitor for unauthorized in-bound traffic
- Demilitarized Zones (DMZ)
- Outside external firewalls
- State of Alabama backbone networks
- Critical subnets

Wireless IDPS may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities.

NBA products can also be deployed if organizations desire additional detection capabilities for denial of service (DoS) attacks, worms, and other threats.

Passive sensors that are performing direct network monitoring should be placed so that they can monitor key network locations, such as the divisions between networks, and key network segments, such as DMZ subnets. Inline sensors are typically intended for network perimeter use, so they would be deployed in close proximity to the perimeter firewalls, either in front to limit incoming attacks that could overwhelm the firewalls or behind the firewall so the IDPS has less traffic to process.

Administrators should ensure that for both passive and inline sensors, IP addresses are not assigned to the network interfaces used to monitor network traffic, except for network interfaces also used for IDPS management. Operating a sensor without IP addresses assigned to its monitoring interfaces is known as operating in "stealth mode."

If monitoring is being performed using a switch SPAN port, it is recommended that the IDS is configured in stealth mode. Stealth mode would not be applicable if the IDS is monitoring from a network tap solution.

The IDPS shall provide near real-time alarms for network-based attacks.

Ensure any unauthorized traffic is logged for further investigation.

4.2 IDPS SECURITY

Create separate accounts for each user and administrator of the IDPS, and assign each account only the necessary privileges.

Configure firewalls, routers, and other packet filtering devices to limit direct access to all IDPS components to only those hosts that need such access.

Ensure that all IDPS management communications are protected appropriately, either through physical (e.g., management network) or logical (e.g., management VLAN) separation, or through encryption of communications. If encryption is used for protection, it shall be performed using a state-approved encryption algorithm (see applicable state IT standard). Many IDPS products encrypt communications using Transport Layer Security (TLS); for products that do not provide sufficient protection through encryption, use a virtual private network (VPN) or other encrypted tunneling method to protect the traffic.

Whenever possible, use strong authentication for remote access to IDPS components, such as two-factor authentication to provide an additional layer of security.

4.3 IDPS ADMINISTRATION

Monitoring the IDPS components for operational and security issues.

Periodically verify that the IDPS is functioning properly (e.g., processing events, alerting appropriately on suspicious activity).

Establish weekly data backup procedures for the IDPS.

Implement anti-virus update procedures for the IDPS.

Perform regular vulnerability assessments.

Respond accordingly to notifications from vendors of security problems with IDPS components (including operating system and non-IDPS applications).

4.3.1 Acquiring and Applying Updates

There are two types of IDPS updates: software updates and signature updates. Software updates fix bugs in the IDPS software or add new functionality, while signature updates add new or refine existing detection capabilities.

Verify the integrity of updates and perform testing before applying them.

Back up configuration settings periodically and before applying software or signature updates to ensure that existing settings are not inadvertently lost.

4.3.2 Tuning and Customization

Review tuning and customizations periodically to ensure that they are still accurate.

Examples of tuning and customization capabilities are thresholds for port scans and application authentication attempts, blacklists and whitelists for host IP addresses and usernames, and alert settings.

A host-based IDPS usually requires considerable tuning and customization. As the host environment changes, ensure that host-based IDPS policies are updated to take those changes into account. Also ensure that significant changes to hosts, such as new hosts and new services, are reflected in NBA settings.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 670-05: Intrusion Detection/Prevention
http://isd.alabama.gov/policy/Policy_670-05_Intrusion_Detection.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 680-03S1: Encryption
http://isd.alabama.gov/policy/Standard_680-03S1_Encryption.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	
Rev A	8/5/2008	Completely revised (based on newer guidance from NIST)